B.E (comp) sem VII 17/12/13
Syst security

25-11-13-DTP16-AK-9

Con.9691-13. **LJ-14237**

(3 Hours) **[Total Marks : 100**

N.B. : (1) Question No. **1** is **compulsory**.
(2) Attempt any **four** questions from the remaining **six** questions.
(3) Figures to the right indicate full marks.
(4) Answer to the questions should be grouped and written together.
(5) Assume any suitable data wherever required but justify the same.

1. (a) Explain substitution cipher and transposition cipher. **5**
   (b) Does a Public Key Infrastructure use symmetric or asymmetric encryption ? Explain your answer. **5**
   (c) What are the system security goals ? Explain why the balance among different goals is needed. **5**
   (d) What are different types of malicious code ? **5**

2. (a) Explain Advanced Encryption Standard Algoritm in detail. **10**

OR

Use the Playfair cipher to encipher the message, "attack cancelled on Monday. Wait for next message". The secret key can be made by filling the first and part of the second row of a matrix with the word "MORNING". Fillng of rest of the matrix can be done with remaining alphabets. Consider alphabets 'Y' and 'Z' together in one cell of the matrix.

   (b) Write a note on Kerberos system that supports authentication in distributed system. **10**

3. (a) Explain control of access to general objects in operating system. **10**
   (b) Explain nonmalicious program errors with examples. **10**

4. (a) If generator g = 2 and n or P = 11, Using Diffie – Hellamn algorithm solve the following :-
      (i) Show that 2 is a primitive root of 11. **4**
      (ii) If A has a public key '9' what is A's private key ? **2**
      (iii) If B has a public key '3' what is B's private key ? **2**
      (iv) Calculate the shared secret key. **2**
   (b) Explain different denial of service attacks. **10**

5. (a) List, explain and compare different kinds of firewalls used for network security. **10**
   (b) Explain multiple levels security model. Also explain multilateral security. **10**

6. Write a detail note on (any **two**) :- **20**
   (a) E-mail security.
   (b) RSA algorithm (Public key algorithm)
   (c) SSL Protocol.
   (d) Covert channel.

7. (a) Explain the process of Digital Certificate generation and the process of evaluation of authenticity of Digital Certificate. **10**
   (b) Explain packet sniffing and packet spoofing. Explain the session hijacking attack. **10**
